K. CONRAD class 1

11 de Julho de 2011

Here we will use factorization to solve Diophantine equations. Let's start by finding the solutions of $x^2 + y^2 = z^2$ in $\mathbb{Z}^+$.

Suppose that $gcd(x, y) = 1$. Then $gcd(x, z) = gcd(y, z) = 1$. z must be odd (because squares mod 4 are 0 ou 1), so x and y have different parity. Without loss of generality, we can assume that x is odd and y is even.

$$x^2 = z^2 - y^2 = \underbrace{(z + y)}_{odd}\underbrace{(z - y)}_{odd} \tag{1}$$

In $\mathbb{Z}$ if $c^2 = ab$ and $\gcd(a, b) = 1$ then $|a|$ and $|b|$ must be squares. Note that we are not sure that a and b are squares (for instance, $6^2 = (-4)(-9)$ and neither -4 nor -9 is a square in $\mathbb{Z}$).
It is easy to show that $\gcd(z + y, z - y)$ can only be 1 or 2. But it cannot be 2 since z is odd and y is even. Now, $z + y, z - y > 0$ and by (1), $z + y = m^2$ and $z - y = n^2$ for some m and n with $\gcd(n, m) = 1$. Then $x = mn$, $y = \frac{m^2-n^2}{2}$ and $z = \frac{m^2+n^2}{2}$. By setting $k = \frac{m+n}{2}$ and $l = \frac{m-n}{2}$ we get $x = k^2 - l^2$, $y = 2kl$ and $z = k^2 + l^2$.

Now we will search integer solutions of the equation

$$y^2 = x^3 - 1 \tag{2}$$

First, rerwrite the equation as $x^3 = y^2 + 1 = (y + i)(y - i)$. In $\mathbb{Z}$, if $c^3 = ab$ and $\gcd(a, b) = 1$ what can we say? a, b must be both cubes (since $-1 = (-1)^3$). Are $y + i$ and $y - i$ relatively prime in the ring $\mathbb{Z}[i]$?

Examples of factorizarions in $\mathbb{Z}[i]$:

$$10 = (3 + i)(3 - i), \quad 3 + 4i = (2 + i)^2$$

In $\mathbb{Z}$ we have trivial factorizations $n = n \cdot 1 = (-n)(-1)$. In $\mathbb{Z}[i]$ trivial factorizations are $\alpha = \alpha \cdot 1 = (-\alpha)(-1) = (i\alpha)(-i) = (-i\alpha)(i)$. We call $\alpha, \beta \in \mathbb{Z}[i]$ relatively prime if their only common factors are $1, -1, i, -i$. In other words, $\gcd(\alpha, \beta) \in U(\mathbb{Z}[i])$, the units of $\mathbb{Z}[i]$.

How can we give examples? Are $1+3i$ and $2+5i$ relatively primes? We define the norm of $\alpha = a+bi \in \mathbb{Z}[i]$ by $Nm(\alpha) = \alpha\overline{\alpha} = a^2+b^2$. The norm is a multiplicative function, that is, $Nm(\alpha\beta) = Nm(\alpha)Nm(\beta)$. So, is δ is a common factor of α and β then $\alpha = \delta\lambda$ and $\beta = \delta\mu$ and so $Nm(\alpha) = Nm(\delta)Nm(\lambda)$ and $Nm(\beta) = Nm(\delta)Nm(\mu)$, this way, we conclude that the norm is a common factor of the norms (in $\mathbb{Z}$). So $1+3i$ and $2+5i$ are relatively prime (the norm of the first one is 10 and the norm of the second is 29 and $\gcd(10,29)=1$).
Warning: In general, if the norms are not relatively prime then it does not mean that the numbers are relatively prime ($1+2i$ and $1-2i$ are an example of this).

We now return to $y^2 = x^3-1$. Let's show that $y+i$ and $y-i$ are relatively prime in $\mathbb{Z}[i]$, for any y fitting the equation $y^2 = x^3-1$.
$Nm(y+i) = Nm(y-i) = y^2+1$. Let $\delta \in \mathbb{Z}[i]$ be a common factor of $y+i$ and $y-i$. Then $\delta|2y$ and $\delta|2i$ in $\mathbb{Z}[i]$. So $Nm(\delta)|4y^2$ and $Nm(\delta)|4$. On the other hand, $Nm(\delta)|Nm(y+i) = y^2+1 = x^3$. Now, we show that x must be odd and y must be even. If x were even then $y^2 \equiv -1 \equiv 7 \mod (8)$ wich is not a square. So x is odd and y e even. Since x^3 is odd and $Nm(\delta)$ divides it and since it also divides 4, we find that $Nm(\delta) = 1$ and so $\delta \in U(\mathbb{Z}[i])$ (note that in $\mathbb{Z}[i]$, $Nm(\delta) = 1$ iff $\delta \in U(\mathbb{Z}[i])$).

If it were the case in $\mathbb{Z}[i]$ that $\alpha\beta = \delta^3$ with α, β being relatively prime implied that α and β are cubes then:

$$y+i = (m+ni)^3 = m(m^2-3n^2)+n(3m^2-n^2)i$$

Thus, $y = n(m^2-3n^2)$ and $1 = n(3m^2-n^2)$ in $\mathbb{Z}$. So $n = \pm 1$ and $1 = \pm(3m^2-1)$. Is must be $1 = -(3m^2-1)$ and $m = 0$. That means that $y = 0$ and $x = 1$ is the only integer solution of (2).

It turns out that since, $\mathbb{Z}[i]$ is a Unique Factorization Domain (UFD), then the above statement is always true. We will show later that this is true. One way to see this in showing that with the norm definded above $\mathbb{Z}[i]$ is an Euclidian Domain.
More generaly, if $\alpha\beta = \gamma^n$ in $\mathbb{Z}[i]$ and α, β are relatively prime then $\alpha = u\mu^n$ and $\beta = v\lambda^n$ where $u, v \in U(\mathbb{Z}[i])$ (this is true for any UFD).

It is easy to show that if $Nm(\alpha) \in \mathbb{P}$ then α is a prime in $\mathbb{Z}[i]$.